CLAIMS

What is claimed is:

1. A method comprising:

applying a block function to a first data input block from a plurality of data input blocks; and

applying the block function to a second data input block from the plurality of data input blocks in accordance with a result of applying the block function to a previous data input block.

2. A method as recited by claim 1, wherein the method is utilized to provide a secure hash function.

3. A method as recited by claim 1, wherein the plurality of data input blocks is formed by dividing an input string.

4. A method as recited by claim 1, wherein each of the plurality of data input blocks has a fixed length.

5. A method as recited by claim 1, wherein one or more of the plurality of data input blocks are padded as needed to provide a fixed length for each of the data input blocks.

6. A method as recited by claim 1, wherein the block function is based on a walk on a graph defined by a plurality of matrices.

7. A method as recited by claim 1, further comprising dividing an input string to provide the plurality of data input blocks.

8. A method as recited by claim 1, further comprising:

dividing an input string to provide the plurality of data input blocks; and

determining a hash value of the input string, the hash value corresponding to a result provided by the application of the block function to a last data input block.

9. A method comprising:

providing a graph corresponding to a data input block;

labeling each outgoing edge of every node in the graph with a label; and

tracing a path through a plurality of labels on the graph, the path being defined by a sequence of elements within the input block.

10. A method as recited by claim 9, wherein the tracing ends at a point that indicates a value of a compression function for a secure hash implementation.

11. A method as recited by claim 9, wherein the graph has a degree *d*.

12. A method as recited by claim 9, wherein the labels are integer labels.

13. A method as recited by claim 12, wherein the graph has a degree *d* and each of the integer labels has a value less than or equal to *d*.

14. A method as recited by claim 9, wherein the input block is a portion of an input string.

15. A method comprising:

constructing a table of entries;

setting an initial matrix to an identity matrix;

processing input data as one or more blocks of fixed length;

indexing each block to a generator matrix represented in the table; and

updating the initial matrix.

16. A method as recited in claim 15, wherein the method is utilized to provide a secure hash function.

17. A method as recited in claim 15, wherein advanced encryption standard (AES) is utilized to provide an inter-block function for the blocks.

18. A method as recited in claim 15, wherein the updating is performed by multiplying the initial matrix by the index matrix.

19. A method as recited in claim 15, wherein the table comprises entries for all possible products of a plurality of generator matrices.

20. A method as recited in claim 15, wherein the generator matrix is a free monoid.

21. One or more computer readable media storing computer executable instructions that, when executed, perform the method as recited in claim 15.

22. A method comprising:

labeling each node of a graph with a matrix;

navigating to a next node of the graph; and

multiplying the node matrix by at least one of a plurality of generator matrices.

23. A method as recited by claim 22, wherein the method is utilized to provide a stream cipher implementation.

24. A method as recited by claim 22, further comprising determining a hash value corresponding to a sequence of intermediate nodes of the graph.

25. A method as recited by claim 22, wherein each of the plurality of generator matrices is a free monoid.

26. One or more computer readable media storing computer executable instructions that, when executed, perform the method as recited in claim 22.

27. A system comprising:

a processor;

a system memory coupled to the processor;

means for applying a block function to a first data input block from a plurality of data input blocks; and

means for applying the block function to a second data input block from the plurality of data input blocks in accordance with a result of applying the block function to a previous data input block.

28. A system as recited by claim 27, wherein the system is utilized to provide at least one item selected from a group comprising a secure hash function and a stream cipher.

29. A system as recited by claim 27, further comprising means for dividing an input string to provide the plurality of data input blocks.

30. A system as recited by claim 27, further comprising:

means for dividing an input string to provide the plurality of data input blocks; and

means for determining a hash value of the input string, the hash value corresponding to a result provided by the application of the block function to a last data input block.

31. One or more computer-readable media having instructions stored thereon that, when executed, direct a machine to perform acts comprising:

applying a block function to a first data input block from a plurality of data input blocks; and

applying the block function to a second data input block from the plurality of data input blocks in accordance with a result of applying the block function to a previous data input block.

32. One or more computer-readable media as recited by claim 31, wherein the method is utilized to provide at least one item selected from a group comprising a secure hash function and a stream cipher.

33. One or more computer-readable media as recited by claim 31, wherein the plurality of data input blocks is formed by dividing an input string.

34. One or more computer-readable media as recited by claim 31, wherein each of the plurality of blocks has a fixed length.

35. One or more computer-readable media as recited by claim 31, wherein one or more of the plurality of data input blocks are padded as needed to provide a fixed length for each of the blocks.

36. One or more computer-readable media as recited by claim 31, wherein the block function is based on a walk on a graph defined by a plurality of matrices.

37. One or more computer-readable media as recited by claim 31, wherein the acts further comprise dividing an input string to provide the plurality of data input blocks.

38. One or more computer-readable media as recited by claim 31, wherein the acts further comprise:

dividing an input string to provide the plurality of data input blocks; and

determining a hash value of the input string, the hash value corresponding to a result provided by the application of the block function to a last data input block.